Practitioner's Docket No. NAI1P482/01.122.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Paul Nicholas Gartside et al.

Application No.: 10/023,852 Group No.: 2131
Filed: December 21, 2001 Examiner: Besrour, Saoussen
For: GENERATING MALWARE DEFINITION DATA FOR MOBILE COMPUTING DEVICES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal, filed in this case on 11/14/2007, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 12/21/2007.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$510.00
Appeal Brief fee due	**$510.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$510.00
Extension fee (if any)	$0.00
TOTAL FEE DUE	**$510.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $510.00 to Deposit Account No. 50-1351 (Order No. NAI1P482).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P482).

Date: January 22, 2008

/KEVINZILKA/
Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Gartside et al.	Group Art Unit: 2131
Application No. 10/023,852	Examiner: Besrour, Saoussen
Filed: 12/21/2001	Atty. Docket No. NAI1P482/01.122.01
For: GENERATING MALWARE DEFINITION DATA FOR MOBILE COMPUTING DEVICES	Date: 01/22/2008

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 11/14/2007, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 12/21/2007.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

VII ARGUMENT

VIII CLAIMS APPENDIX

IX EVIDENCE APPENDIX

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, an appeal noted on 06/06/2007 in application serial number 10/122,087 may be, but is not necessarily, related.

Since no decision(s) has been rendered in such proceeding(s), no material is included in the Related Proceedings Appendix appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 3-6, 8-17, 19-22, 24-33, 35-38, 40-47, 49 and 50

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 3-6, 8-17, 19-22, 24-33, 35-38, 40-47, 49 and 50
3. Claims allowed: None
4. Claims rejected: 1, 3-6, 8-17, 19-22, 24-33, 35-38, 40-47, 49 and 50
5. Claims cancelled: 2, 7, 18, 23, 34, 39 and 48

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 3-6, 8-17, 19-22, 24-33, 35-38, 40-47, 49 and 50

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, the Amendment submitted on 03/13/2006 was not entered by the Examiner.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 3-5 et al., a computer program product embodied on a tangible computer readable medium is provided for controlling a computer to generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device. Obtaining code is included that is operable to obtain from a data source master malware definition data (e.g. see item 34 of Figure 3, etc.), the master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat. In addition, identifying code is included that is operable to identify one or more classes of malware threat against which the mobile computing device is to be protected (e.g. see item 40 of Figure 3, etc.). Furthermore, generating code is included that is operable to generate from the master malware definition data the mobile computing device malware definition data, the mobile computing device malware definition data identifying items of malware identified within the master malware definition data which are within classes of malware threat against which the mobile computing device is to be protected (e.g. see item 42 of Figure 3, etc.).

Still yet, the obtaining code, the identifying code and the generating code are executed by a fixed location computing device (e.g. see item 36 of Figure 3, etc.), the fixed location computer being operable to transfer to the mobile computing device one or more computer files including at least a computer file containing the mobile computer device malware definition data (e.g. see item 64 of Figure 5, etc.). Additionally, the fixed location computing device stores profile data identifying one or more different types of mobile computing device to which the fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of the mobile computing devices is vulnerable (e.g. see item 46 of Figure 4, etc.). Moreover, only a subset of the master malware definition data is used to generate the mobile computing device malware definition data for tailoring the mobile computing device malware definition data to accommodate malware threats to which the mobile computing device is vulnerable. Further, the one or more classes of malware threat against which the mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to the mobile computing device, and classes for which it is desired to protect the mobile computing device according to user defined policies. See, for

example, Page 3, line 26-Page 4, line 5; Page 4, lines 13-17, 20-21 and 25-28; Page 5, lines 12-17; and Page 11, lines 3-7 et al.

With respect to a summary of Claim 17, as shown in Figures 3-5 et al., a method of generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device is provided. In use, master malware definition data is obtained from a data source (e.g. see item 34 of Figure 3, etc.), the master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat. Additionally, one or more classes of malware threat against which the mobile computing device is to be protected are identified (e.g. see item 40 of Figure 3, etc.). Furthermore, the mobile computing device malware definition data is generated from the master malware definition data, the mobile computing device malware definition data identifying items of malware identified within the master malware definition data which are within classes of malware threat against which the mobile computing device is to be protected (e.g. see item 42 of Figure 3, etc.).

Still yet, the steps of obtaining, identifying and generating are performed by a fixed location computing device (e.g. see item 36 of Figure 3, etc.), the fixed location computer being operable to transfer to the mobile computing device one or more computer files including at least a computer file containing the mobile computer device malware definition data (e.g. see item 64 of Figure 5, etc.). Additionally, the fixed location computing device stores profile data identifying one or more different types of mobile computing device to which the fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of the mobile computing devices is vulnerable (e.g. see item 46 of Figure 4, etc.). Moreover, only a subset of the master malware definition data is used to generate the mobile computing device malware definition data for tailoring the mobile computing device malware definition data to accommodate malware threats to which the mobile computing device is vulnerable. Further, the one or more classes of malware threat against which the mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to the mobile computing device, and classes for which it is desired to protect the mobile computing device according to user defined policies. See, for example, Page 3, line 26-

Page 4, line 5; Page 4, lines 13-17, 20-21 and 25-28; Page 5, lines 12-17; and Page 11, lines 3-7 et al.

With respect to a summary of Claim 33, as shown in Figures 3-5 et al., an apparatus is provided for generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device. Obtaining logic is included that is operable to obtain from a data source master malware definition data (e.g. see item 34 of Figure 3, etc.), the master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat. In addition, identifying logic is included that is operable to identify one or more classes of malware threat against which the mobile computing device is to be protected (e.g. see item 40 of Figure 3, etc.). Furthermore, generating logic is included that is operable to generate from the master malware definition data the mobile computing device malware definition data, the mobile computing device malware definition data identifying items of malware identified within the master malware definition data which are within classes of malware threat against which the mobile computing device is to be protected (e.g. see item 42 of Figure 3, etc.).

Still yet, the obtaining logic, the identifying logic and the generating logic are provided by a fixed location computing device (e.g. see item 36 of Figure 3, etc.), the fixed location computer being operable to transfer to the mobile computing device one or more computer files including at least a computer file containing the mobile computer device malware definition data (e.g. see item 64 of Figure 5, etc.). Additionally, the fixed location computing device stores profile data identifying one or more different types of mobile computing device to which the fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of the mobile computing devices is vulnerable (e.g. see item 46 of Figure 4, etc.). Moreover, only a subset of the master malware definition data is used to generate the mobile computing device malware definition data for tailoring the mobile computing device malware definition data to accommodate malware threats to which the mobile computing device is vulnerable. Further, the one or more classes of malware threat against which the mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to the mobile computing device, and classes for which it is desired to protect the mobile computing device according to user defined policies. See, for

example, Page 3, line 26-Page 4, line 5; Page 4, lines 13-17, 20-21 and 25-28; Page 5, lines 12-17; and Page 11, lines 3-7 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1, 3-6, 8-17, 19-22, 24-33, 35-38, 40-47, 49 and 50 under 35 U.S.C. 103(a) as being unpatentable over Nambu (U.S. Patent No. 2002/0124181), in view of Hershberg et al. (U.S. Patent No. 2003/0022657).

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1, 3-6, 8-17, 19-22, 24-33, 35-38, 40-47, 49 and 50 under 35 U.S.C. 103(a) as being unpatentable over Nambu (U.S. Patent No. 2002/0124181), in view of Hershberg et al. (U.S. Patent No. 2003/0022657).

Group #1: Claims 1, 3, 9, 12, 15-17, 19, 25, 28, 31-33, 35, 41 and 44

With respect to the independent claims, the Examiner has relied on the following excerpts from the Nambu reference to make a prior art showing of appellant's claimed "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

> "In accordance with the circumstances under which viruses are generated, the maintenance server 41 registers and manages the information of new types of viruses. The information of the new virus includes, for example, virus name, danger level, discovery data, vaccine manufacture date (vaccine manufacture schedule), and the corresponding pattern file name (pattern number). The maintenance server 41 receives and stores updated vaccine software (including scan engines) and pattern data files that are provided by each company.
>
> The support computers 42a, 42b of the vaccine software makers may upload vaccine software and pattern files to the maintenance server 41.
>
> The maintenance server 41 is connected to various user terminals (in FIG. 5, four terminals) 45a, 45b, 45c, 45d by a public line 46, which includes the internet. The first terminal 45a is, for example, a cellular phone, and the second terminal 45b is, for example, a portable terminal such as a personal digital assistant (PDA) The third terminal 45c is, for example, a computer system of a personal computer, and the fourth terminal 45d is for example, a game device of a home communication terminal (set-top box) provided with a communication function." (paragraphs [0072]-[0074] - emphasis added)

More specifically, the Examiner has argued that "it is known within existing malware definition data to include information that classifies the malware items using classes." However, appellant respectfully disagrees and notes that the above excerpts relied on by the Examiner merely teach that a "maintenance server... registers and manages the information of new types of viruses" and that "[t]he maintenance server... receives and stores updated vaccine software (including scan engines) and pattern data files" (paragraph [0072] – emphasis added). Further, the excerpts teach that "support computers... of the vaccine software makers may upload vaccine software and pattern files to the maintenance server" and that [t]he maintenance server... is connected to various user terminals" (paragraphs [0073]-[0074] – emphasis added).

However, registering and managing new virus types, receiving and storing updated vaccine software and pattern data files, and uploading vaccine software to a server which is connected to user terminals, as in Nambu, does not teach "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by appellant. Additionally, it appears that the Examiner has relied on an inherency argument regarding the above emphasized claim limitations. In view of the arguments made hereinabove, any such inherency argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested (See MPEP 2112).

Additionally, in response, appellant asserts that the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraph [0071] in Nambu "states that the pattern files can be referred to as signature files or virus definition files, where it is a code of particular virus, [which is] interpreted by [the] examiner as the class of malware." The Examiner has also argued that paragraphs [0075]-[0078] state "that the maintenance server stores information on all the related user terminals based on the user-related information" and that "it provides the terminals with updated vaccine and pattern files." Further, the Examiner has argued that paragraph [0083] "discloses protecting against the new virus, which the device is to be protected against," that paragraph [0089] "states that the information 54a and 54b...include information of the user's device, such as applied pattern name for that user device," and that paragraph [0095] "states that the new anti-virus program reads user information and acquires the software related information from each use[r], including [the] pattern file."

Appellant respectfully disagrees and asserts that paragraph [0071] in Nambu only discloses pattern files which may be referred to as signature files and virus definition files, where such pattern files are each associated with a new virus (see paragraph [0072]). Further, the Examiner has even admitted that Nambu teaches "a code of a particular virus," as noted above. Clearly, a pattern file that is associated with a particular virus, as in Nambu, does not meet appellant's claimed "one or more classes of malware" (emphasis added), as claimed. Additionally, appellant respectfully asserts that merely "install[ing]... pattern files...[to prevent] the terminal from being infected by the new virus" (paragraph [0083]), as relied on by the Examiner, fails to specifically teach "identifying one or more classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed.

Additionally, with respect to the independent claims, the Examiner has relied on the following excerpts from the Nambu reference to make a prior art showing of appellant's claimed "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (see this or similar, but not necessarily identical language in the independent claims).

> "The maintenance server 41 stores information related to the user terminals 45a-45d and, based on the user-related information, provides

> the terminals 45a-45d with updated vaccine software and pattern files." (paragraph [0075] - emphasis added)
>
> "The maintenance server 41 includes a new anti-virus processing program 51, a resource distribution program 52, and information files 53, 54. The maintenance server 41 stores vaccine software and pattern files 55, 56 that are received from the vaccine software makers.
>
> The new anti-virus processing program 51 includes a new virus information processing program 51a and a user information processing program 51b. The first information file 53 functions as a new virus countering information memory and stores vaccine software information (name of virus for which a vaccine has been produced, name of pattern file of virus for which a vaccine has been produced, name of virus for which a vaccine has not yet been produced, and danger level). The second information file 54 functions as a user information memory. The file 54 stores the present condition of the user terminal (information indicating the presently used vaccine software and whether to constantly update the vaccine software (including that of other manufacturers))." (paragraphs [0077]-[0078] - emphasis added)

Appellant respectfully points out that the above excerpts relied on by the Examiner merely teach that a "maintenance server... stores information related to the user terminals" and "provides the terminals... with updated vaccine software and pattern files" (emphasis added). Additionally, the excerpts teach that "[t]he maintenance server 41 stores vaccine software and pattern files" (emphasis added). Further, the excerpts teach that "[t]he first information file... functions as a new virus countering information memory and stores vaccine software information" and that "[t]he second information file... stores the present condition of the user terminal" (emphasis added).

However, merely storing vaccine software and pattern files and information, in addition to storing the present condition of a user terminal, as in Nambu, fails to disclose "generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed by appellant. Clearly, merely storing pattern files and information, as in Nambu, simply fails to even suggest "classes of malware threat against which said mobile computing device is to be protected" (emphasis added), in the manner as claimed by appellant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraphs [0093], [0095] and [0096] state "software designated information from each user." Appellant respectfully disagrees. First, appellant respectfully asserts that simply alleging that the Nambu reference discloses "information from each user," as noted by the Examiner, fails to even suggest "classes of malware threat," as appellant claims. Second, appellant respectfully asserts that simply disclosing "stor[ing] various types of information" (paragraph [0093]), "software-related information from each user (e.g., hardware information, identification number, vaccine software information, designation of applied vaccine, applied pattern file name)" (paragraph [095]), and that "pattern files may be provided" (paragraph [0096]), as in Nambu, fails to even suggest "classes of malware threat against which said mobile computing device is to be protected" (emphasis added), as claimed. As noted above, a pattern file in Nambu only relates to a particular virus, and thus does not meet appellant's claimed "classes of malware threat" (emphasis added), as claimed.

Further, with respect to the independent claims, the Examiner has relied on paragraphs [0074], [0075], and [0077] from the Nambu reference (reproduced above) to make a prior art showing of appellant's claimed technique "wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (see this or similar, but not necessarily identical language in the independent claims).

Appellant respectfully notes that the above reference excerpts relied on by the Examiner merely disclose that "[t]he maintenance server... is connected to various user terminals" (paragraph [0074] – emphasis added), that "[t]he maintenance server 41 stores information related to the user terminals" (paragraph [0075] – emphasis added), and that "[t]he maintenance server... stores vaccine software and pattern files... that are received from the vaccine software makers" (paragraph [0077] – emphasis added).

However, merely storing information related to user terminals, in addition to storing vaccine software and pattern files, as in Nambu, fails to teach a technique "wherein said fixed

location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by appellant. Clearly, storing information relating to user terminals and providing updated vaccine software and pattern files, as in Nambu, simply fails to suggest "transfer[ing] computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by appellant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraph [0083] in Nambu "states transferring vaccine software and pattern file." Appellant respectfully disagrees. As argued above, appellant respectfully asserts that the pattern file in Nambu only relates to a particular virus (see paragraph [0072]), which simply does not even suggest "transfer[ing] computer files and corresponding threat data identifying one or more classes of malware threat," especially where such classes of malware threat particularly include those "to which each of said mobile computing devices is vulnerable" (emphasis added), as claimed by appellant.

Further still, with respect to the independent claims, the Examiner has relied on paragraph [0078] (reproduced above), in addition to the following excerpts, from the Nambu reference to make a prior art showing of appellant's claimed technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (see this or similar, but not necessarily identical language in the independent claims). Specifically, the Examiner has stated "acquiring vaccine via user information processing program which determined condition of the user terminal."

> "The new anti-virus processing program 51 acquires the vaccine software-related information from the second information file 54 via the user information processing program 51b. The processing program 51 acquires the new virus countering information that corresponds to the vaccine software-related information from the first information file 53 via the new virus information processing program 51a." (paragraph [0081] - emphasis added)

> "The maintenance server 41 determines whether the vaccine software and pattern data files presently used by the user terminals 45a-45d are capable of countering a new virus from the countering information file 53 and the user-related information file 54. Based on the determination, the resource distribution program 52 distributes to the user terminals 45a-45d, vaccine software and pattern files (including that of other makers) that have been updated to counter the new virus." (paragraph [0108] - emphasis added)

Appellant respectfully disagrees and points out that the above excerpts relied on by the Examiner merely disclose that "[t]he first information file... functions as a new virus countering information memory and stores vaccine software information" and that "[t]he second information file... stores the present condition of the user terminal" (paragraph [0078] - emphasis added). Additionally, the above excerpts teach that the "new anti-virus processing program... acquires the vaccine software-related information" as well as "new virus countering information." Further, the excerpts teach that "[t]he maintenance server... determines whether the vaccine software and pattern data files presently used... are capable of countering a new virus" and that "[b]ased on the determination, the resource distribution program... distributes to the user terminals... vaccine software and pattern files... that have been updated to counter the new virus" (emphasis added).

However, merely acquiring vaccine and virus countering information, determining whether a vaccine is capable of countering a new virus, and distributing vaccine software based on the determination, as in Nambu, fails to suggest a technique "wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies" (emphasis added), as claimed by appellant. Clearly, distributing vaccine software based on the determination if the vaccine is capable of countering a new virus, as in Nambu, simply fails to even suggest that "one or more classes of malware threat... are chosen according to classes of malware threat known to pose a problem to said mobile computing device" (emphasis added), in the manner as claimed by appellant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraphs [0089] and [0100]-[0103] in Nambu state "determining that the vaccine software and data pattern file

have not been updated for new virus, then based on the determination obtaining up to date vaccine from user information."

Appellant respectfully disagrees. Paragraphs [0089] and [0100]-[0103] in Nambu, as relied on by the Examiner, merely relate to "information of the user's terminal, such as...designation of applied vaccine" which designates whether "user A wishes to receive updated vaccine, which includes that of other makers" (see paragraph [0089]), such that if "user A wishes to obtain the most updated vaccine (including that of other makers)...countering information...of the B vaccine software maker [is read]" (see paragraph [0103]). Clearly, simply determining whether a user wishes to receive an updated vaccine from another vaccine software maker, as in Nambu, fails to even relate to "classes of malware threat" (emphasis added), let alone specifically teach "one or more classes of malware threat... are chosen according to classes of malware threat **known to pose a problem to said mobile computing device**" (emphasis added), in the manner as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 4, 6, 20, 22, 36 and 38

With respect to Claim 4 et al., the Examiner has relied on paragraphs [0074], [0075], and [0077] from the Nambu reference to make a prior art showing of appellant's claimed technique

"wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized."

Appellant respectfully notes that the above excerpts relied on by the Examiner merely teach that a "maintenance server... is connected to various user terminals" and that "[t]he maintenance server... stores information related to the user terminals... and, based on the user-related information, provides the terminals... with updated vaccine software" (paragraph [0074]). Also, the above excerpts teach that "[t]he maintenance server... stores vaccine software and pattern files... that are received from the vaccine software makers" (paragraph [0077] – emphasis added).

However, merely teaching that a maintenance server is connected to user terminals, stores vaccine files received from vaccine software makers, and provides the terminals with updated vaccine software, as in Nambu, fails to suggest a technique "wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized" (emphasis added), as claimed by appellant. Clearly, vaccine files received from vaccine software markers, as in Nambu, simply fails to even suggest that "different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized" (emphasis added), as claimed by appellant.

In the Office Action mailed 08/15/2007, the Examiner failed to respond to appellant's above arguments. Thus, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #3: Claims 5, 21 and 37

With respect to Claim 5 et al., the Examiner has relied on paragraphs [0075] and [0077] in Nambu to make a prior art showing of appellant's claimed "wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization."

Appellant respectfully asserts that paragraph [0075] from Nambu merely discloses that "[t]he maintenance server 41 stores information related to the user terminals 45a-45d and, based on the user-related information, provides the terminals 45a-45d with updated vaccine software and pattern files." In addition, paragraph [0077] from Nambu simply discloses that "[t]he maintenance server 41 stores vaccine software and pattern files 55, 56 that are received from the vaccine software makers."

However, merely teaching that a maintenance server provides user terminals with updated vaccine software and pattern files and receives vaccine software and pattern files from the vaccine software makers, as in Nambu, fails to specifically disclose that "said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #4: Claims 8, 24 and 40

With respect to Claim 8 et al., the Examiner has relied on the following excerpt from the Nambu reference to make a prior art showing of appellant's claimed technique "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data."

> "When the vaccine software used by the presently connected user terminal does not correspond to the new virus and the user wishes to constantly update the vaccine software (including that of other manufacturers), the new anti-virus processing program 51 provides the resource distribution program 52 with information for sending vaccine software corresponding to the new virus to the user terminal." (paragraph [0082])

Appellant respectfully notes that the above excerpt relied on by the Examiner merely discloses that "[w]hen the vaccine software used by the presently connected user terminal does not correspond to the new virus and the user wishes to constantly update the vaccine software" the "anti-virus processing program... provides the resource distribution program... with information for sending vaccine software corresponding to the new virus to the user terminal" (emphasis added).

However, the mere disclosure of the user wishing to constantly update the vaccine software, in addition to the resource distribution program sending vaccine software to the user terminal, as in Nambu, does not teach a technique "wherein user controlled policy data is used in combination with said threat data to control against which classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data" (emphasis added), as claimed by appellant. Clearly, sending vaccine software to the user terminal when the vaccine software used by the user terminal does not correspond to the new virus, as in Nambu, simply fails to even suggest "control[ling] against which classes of malware threat said mobile computing device is protected" (emphasis added), in the manner as claimed by appellant.

In the Office Action mailed 08/15/2007, the Examiner has argued that paragraphs [0089] and [0100]-[0103] from Nambu "states determining that the vaccine software and data pattern file have not been updated for new virus, then based on the determination obtaining up to date vaccine from user information."

Appellant respectfully disagrees. Paragraph [0089] from Nambu simply discloses that "[t]he information 54a, 54b respectively include information of the user's terminal, such as hardware information, identification number, vaccine software information, designation of applied vaccine, and applied pattern file name." Clearly, only disclosing information of a user's

terminal, as in Nambu, fails to teach that "user controlled policy data is used in combination with said threat data to **control** against **which classes** of malware threat said mobile computing device is protected by said mobile computing device malware definition data" (emphasis added), as claimed.

In addition, paragraphs [0100]-[0103] from Nambu disclose that "based on the vaccine software information included in the user-related information 54a, the anti-virus processing program 51 recognizes that the provider of the vaccine software used by the user A terminal (cellular phone) 45a is vaccine software maker A" (paragraph [0101]), that "the new anti-virus processing program 51 acquires information that the user A wishes to obtain the most updated vaccine (including that of other makers) from the user-related information 54a of user A," and that "[b]ased on the information, the anti-virus processing program 51 reads the countering information 53b (FIG. 6) of the B vaccine software maker from the first information file 53 by means of the new anti-virus information processing program 51a" (paragraph [0103]).

Thus, such paragraphs from Nambu only disclose that user-related information indicates that an associated user wishes to obtain the most updated vaccine including that of other makers, and that based on such information the anti-virus processing program reads countering information of a B vaccine software maker. Clearly, such teaching does not specifically teach "user controlled policy data [that] is used in combination with said threat data to **control** against **which classes** of malware threat said mobile computing device is protected by said mobile computing device malware definition data" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #5: Claims 10, 26 and 42

With respect to Claim 10 et al., the Examiner has relied on paragraph [0078] from Nambu to make a prior art showing of appellant's claimed technique "wherein said fixed location computer device detects to which mobile computing devices it transfers computer files

by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices."

Appellant respectfully asserts that the excerpt from Nambu relied on by the Examiner merely discloses that the "new anti-virus processing program 51 includes a new virus information processing program 51a and a user information processing program 51b," and that "[t]he first information file 53 functions as a new virus countering information memory and stores vaccine software information."

Clearly, merely disclosing a new virus information processing program and a user information processing program, in addition to a first information file that stores vaccine software information, as in Nambu, fails to even suggest a technique "wherein said fixed location computer device detects to which mobile computing devices it transfers computer files **by detecting installation** upon said fixed location computing device **of one or more transfer controlling computer programs** operable to control transfer of computer files to one or more predetermined mobile computing devices" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #6: Claims 11, 13, 27, 29, 43 and 45

With respect to Claim 11 et al., the Examiner has relied on paragraph [0078] from Nambu to make a prior art showing of appellant's claimed technique "wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device."

Appellant respectfully asserts that such excerpt from Nambu relied on by the Examiner simply discloses that the "new anti-virus processing program 51 includes a new virus information processing program 51a and a user information processing program 51b," and that

"[t]he first information file 53 functions as a new virus countering information memory and stores vaccine software information."

However, simply disclosing a new virus information processing program and a user information processing program, in addition to a first information file that stores vaccine software information, as in Nambu, fails to even suggest that a "fixed location computing device also transfers a **malware scanner computer program** from said data source to said mobile computing device" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #7: Claims 14, 30 and 46

The Examiner has relied on paragraph [0112] from Nambu to make a prior art showing of appellant's claimed technique "wherein said master malware definition data is also used to protect said fixed location computing device from malware."

Appellant respectfully asserts that such excerpt from Nambu relied on by the Examiner merely discloses that "[t]he maintenance server 41 may provide one or more vaccine software and pattern files from three or more vaccine software makers...[or] may provide the maintenance server 41 with a plurality of vaccine software and pattern files from a single vaccine software maker."

However, simply disclosing that a maintenance server provides vaccine software and pattern files from three or more vaccine software makers and that the maintenance server may alternatively provide the maintenance server with a plurality of vaccine software and pattern files from a single vaccine software maker, as in Nambu, fails to specifically teach that "said master malware definition data is also used to protect said fixed location computing device from malware" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #8: Claim 47

The Examiner has relied on paragraphs [0074], [0075] and [0083] from Nambu to make a prior art showing of appellant's claimed technique "wherein said fixed location device stores policy data including user defined settings identifying the manner in which said profile data is to be interpreted."

Appellant respectfully asserts that such excerpts merely disclose that "[t]he maintenance server 41 is connected to various user terminals" (paragraph [0074]) and that such maintenance server "stores information related to the user terminals 45a-45d and, based on the user-related information, provides the terminals 45a-45d with updated vaccine software and pattern files" (paragraph [0075]). Further, the excerpts disclose "install[ing] updated vaccine software and pattern files in the user terminal" (paragraph [0083]).

However, simply disclosing a maintenance server that is connected to user terminals and installs updated vaccine software and pattern files on the user terminals based on information related to the user terminals, as in Nambu fails to meet appellant's claimed technique "wherein said fixed location device stores policy data including user defined settings identifying the manner in which said profile data **is to be interpreted**" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #9: Claim 49

The Examiner has relied on paragraphs [0100]-[0103] from Nambu to make a prior art showing of appellant's claimed technique "wherein said one or more classes of malware threat

against which said mobile computing device is to be protected are chosen according to said classes of malware threat known to pose a problem to an operating system of said mobile computing device."

Appellant respectfully asserts that paragraphs [0100]-[0103] from Nambu simply disclose that "based on the vaccine software information included in the user-related information 54a, the anti-virus processing program 51 recognizes that the provider of the vaccine software used by the user A terminal (cellular phone) 45a is vaccine software maker A" (paragraph [0101]), that "the new anti-virus processing program 51 acquires information that the user A wishes to obtain the most updated vaccine (including that of other makers) from the user-related information 54a of user A," and that "[b]ased on the information, the anti-virus processing program 51 reads the countering information 53b (FIG. 6) of the B vaccine software maker from the first information file 53 by means of the new anti-virus information processing program 51a" (paragraph [0103]).

Thus, such paragraphs from Nambu only disclose that user-related information indicates that an associated user wishes to obtain the most updated vaccine including that of other makers, and that based on such information the anti-virus processing program reads countering information of a B vaccine software maker. Clearly, such teaching does not even suggest that "said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to said classes of malware threat known to pose a problem to an **operating system** of said mobile computing device" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #10: Claim 50

The Examiner has relied on paragraphs [0100]-[0103] from Nambu to make a prior art showing of appellant's claimed technique "wherein at least a portion of said mobile computing device malware definition data poses a problem only to said mobile computing device and not to said fixed location computing device."

Appellant respectfully asserts that paragraphs [0100]-[0103] from Nambu simply disclose that "based on the vaccine software information included in the user-related information 54a, the anti-virus processing program 51 recognizes that the provider of the vaccine software used by the user A terminal (cellular phone) 45a is vaccine software maker A" (paragraph [0101]), that "the new anti-virus processing program 51 acquires information that the user A wishes to obtain the most updated vaccine (including that of other makers) from the user-related information 54a of user A," and that "[b]ased on the information, the anti-virus processing program 51 reads the countering information 53b (FIG. 6) of the B vaccine software maker from the first information file 53 by means of the new anti-virus information processing program 51a" (paragraph [0103]).

Thus, such paragraphs from Nambu only disclose that user-related information indicates that an associated user wishes to obtain the most updated vaccine including that of other makers, and that based on such information the anti-virus processing program reads countering information of a B vaccine software maker. Clearly, such teaching does not teach that "at least a portion of said mobile computing device malware definition data poses a problem **only** to said mobile computing device and not to said fixed location computing device" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product embodied on a tangible computer readable medium for controlling a computer to generate mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said computer program product comprising:

obtaining code operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying code operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating code operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected;

wherein said obtaining code, said identifying code and said generating code are executed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data;

wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable;

wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable;

wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies.

2. (Cancelled)

3. (Previously Presented) A computer program product as claimed in claim 1, wherein said fixed location computing device is a user computer having communication link with said mobile computing device.

4. (Previously Presented) A computer program product as claimed in claim 1, wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized.

5. (Previously Presented) A computer program product as claimed in claim 4, wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization.

6. (Original) A computer program product as claimed in claim 4, when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and, if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device.

7. (Cancelled)

8. (Previously Presented) A computer program product as claimed in claim 1, wherein user controlled policy data is used in combination with said threat data to control against which

classes of malware threat said mobile computing device is protected by said mobile computing device malware definition data.

9. (Previously Presented) A computer program product as claimed in claim 1, wherein said different types of mobile computing device correspond to different types of operating system computer programs used by mobile computing devices.

10. (Previously Presented) A computer program product as claimed in claim 1, wherein said fixed location computer device detects to which mobile computing devices it transfers computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices.

11. (Previously Presented) A computer program product as claimed in claim 1, wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device.

12. (Previously Presented) A computer program product as claimed in claim 1, wherein said fixed location computing device checks for updated master malware definition data becoming available from said data source and, if such updated master malware definition data becomes available, then repeats said steps of obtaining, identifying and generating.

13. (Original) A computer program product as claimed in claim 11, wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

14. (Previously Presented) A computer program product as claimed in claim 1, wherein said master malware definition data is also used to protect said fixed location computing device from malware.

15. (Previously Presented) A computer program product as claimed in claim 1, wherein said fixed location computing device is connected to said data source by a fixed internet link.

16. (Original) A computer program product as claimed in claim 1, wherein said items of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

17. (Previously Presented) A method of generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said method comprising the steps of:

obtaining from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying one or more classes of malware threat against which said mobile computing device is to be protected; and

generating from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected;

wherein said steps of obtaining, identifying and generating are performed by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data;

wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable;

wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable;

wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies.

18. (Cancelled)

19. (Previously Presented) A method as claimed in claim 17, wherein said fixed location computing device is a user computer having communication link with said mobile computing device.

20. (Previously Presented) A method as claimed in claim 17, wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized.

21. (Previously Presented) A method as claimed in claim 20, wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization.

22. (Original) A method as claimed in claim 20, when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and, if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device.

23. (Cancelled)

24. (Previously Presented) A method as claimed in claim 17, wherein user controlled policy data is used in combination with said threat data to control against which classes of malware

threat said mobile computing device is protected by said mobile computing device malware definition data.

25. (Previously Presented) A method as claimed in claim 17, wherein said different types of mobile computing device correspond to different types of operating system computer programs used by mobile computing devices.

26. (Previously Presented) A method as claimed in claim 17, wherein said fixed location computer device detects to which mobile computing devices it transfers computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices.

27. (Previously Presented) A method as claimed in claim 17, wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device.

28. (Previously Presented) A method as claimed in claim 17, wherein said fixed location computing device checks for updated master malware definition data becoming available from said data source and, if such updated master malware definition data becomes available, then repeats said steps of obtaining, identifying and generating.

29. (Original) A method as claimed in claim 27, wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

30. (Previously Presented) A method as claimed in claim 17, wherein said master malware definition data is also used to protect said fixed location computing device from malware.

31. (Previously Presented) A method as claimed in claim 17, wherein said fixed location computing device is connected to said data source by a fixed internet link.

32. (Original) A method as claimed in claim 17, wherein said items of malware include one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

33. (Previously Presented) Apparatus for generating mobile computing device malware definition data for use by a mobile computing device malware scanner executable upon a mobile computing device, said apparatus comprising:

obtaining logic operable to obtain from a data source master malware definition data, said master malware definition identifying a plurality of items of malware each belonging to one of a plurality of classes of malware threat;

identifying logic operable to identify one or more classes of malware threat against which said mobile computing device is to be protected; and

generating logic operable to generate from said master malware definition data said mobile computing device malware definition data, said mobile computing device malware definition data identifying items of malware identified within said master malware definition data which are within classes of malware threat against which said mobile computing device is to be protected;

wherein said obtaining logic, said identifying logic and said generating logic are provided by a fixed location computing device, said fixed location computer being operable to transfer to said mobile computing device one or more computer files including at least a computer file containing said mobile computer device malware definition data;

wherein said fixed location computing device stores profile data identifying one or more different types of mobile computing device to which said fixed location computing device transfers computer files and corresponding threat data identifying one or more classes of malware threat to which each of said mobile computing devices is vulnerable;

wherein only a subset of said master malware definition data is used to generate said mobile computing device malware definition data for tailoring said mobile computing device malware definition data to accommodate malware threats to which said mobile computing device is vulnerable;

wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to classes of malware threat known to pose a problem to said mobile computing device, and classes for which it is desired to protect said mobile computing device according to user defined policies.

34. (Cancelled)

35. (Previously Presented) An apparatus as claimed in claim 33, wherein said fixed location computing device is a user computer having communication link with said mobile computing device.

36. (Previously Presented) An apparatus as claimed in claim 33, wherein, when said mobile computing device is connected to said fixed location computing device, different versions of user generated computer files respectively stored by said mobile computing device and said fixed location computing device are synchronized.

37. (Previously Presented) An apparatus as claimed in claim 36, wherein said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device during said synchronization.

38. (Previously Presented) An apparatus as claimed in claim 36, when said mobile computing device is connected to said fixed location computing device, versions of said mobile computing device malware definition data stored on said mobile computing device and said fixed location computing device are compared, and, if said fixed location computing device has a more up-to-date version of said mobile computing device malware definition data, then said more up-to-date version of said mobile computing device malware definition data is transferred from said fixed location computing device to said mobile computing device.

39. (Cancelled)

40. (Previously Presented) An apparatus as claimed in claim 33, wherein user controlled policy data is used in combination with said threat data to control against which classes of

malware threat said mobile computing device is protected by said mobile computing device malware definition data.

41. (Previously Presented) An apparatus as claimed in claim 33, wherein said different types of mobile computing device correspond to different types of operating system computer programs used by mobile computing devices.

42. (Previously Presented) An apparatus as claimed in claim 33, wherein said fixed location computer device detects to which mobile computing devices it transfers computer files by detecting installation upon said fixed location computing device of one or more transfer controlling computer programs operable to control transfer of computer files to one or more predetermined mobile computing devices.

43. (Previously Presented) An apparatus as claimed in claim 33, wherein fixed location computing device also transfers a malware scanner computer program from said data source to said mobile computing device.

44. (Previously Presented) An apparatus as claimed in claim 33, wherein said fixed location computing device checks for updated master malware definition data becoming available from said data source and, if such updated master malware definition data becomes available, then repeats said steps of obtaining, identifying and generating.

45. (Previously Presented) An apparatus as claimed in claim 43, wherein said fixed location computing device checks for an updated malware scanner computer program becoming available from said data source and, if such an updated malware scanner computer program become available, then obtains said updated malware scanner computer program for transfer to said mobile computing device.

46. (Previously Presented) An apparatus as claimed in claim 33, wherein said master malware definition data is also used to protect said fixed location computing device from malware.

47. (Previously Presented) The computer program product as claimed in claim 1, wherein said fixed location device stores policy data including user defined settings identifying the manner in which said profile data is to be interpreted.

48. (Cancelled)

49. (Previously Presented) A computer program product as claimed in claim 1, wherein said one or more classes of malware threat against which said mobile computing device is to be protected are chosen according to said classes of malware threat known to pose a problem to an operating system of said mobile computing device.

50. (Previously Presented) A computer program product as claimed in claim 1, wherein at least a portion of said mobile computing device malware definition data poses a problem only to said mobile computing device and not to said fixed location computing device.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

Since no decision(s) has been rendered in such proceeding(s), no material is included in this Related Proceedings Appendix.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P482).

Respectfully submitted,

By: /KEVINZILKA/ Date: January 22, 2008
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660